Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	CG Docket No. 17-59
	)	
	)	
	)	
To: The Commission	)	

COMMENTS OF ZipDX

Further Notice of Proposed Rulemaking – FCC 17-151

David Frankel
dfrankel@zipdx.com
17554 Via Sereno
Monte Sereno, CA 95030
Tel: 800-372-6535

Filed: January 22, 2018

ZipDX responds herein to the specific questions raised in the FNPRM (FCC 17-151). With respect to erroneously blocked calls, we reiterate comments made in our original Comments to the NPRM which directly address this issue. With respect to reporting requirements, we reference our previously submitted ex parte comments pertaining to *originating* providers. With respect to other data sources, we highlight the FTC and YouMail efforts. We highlight again that current efforts by FCC and industry are not the best use of resources to combat this problem.

From the FNPRM[1]: "[W]e seek comment on potential mechanisms to ensure that erroneously blocked calls can be unblocked as quickly as possible and without undue harm to callers and consumers."

Recognizing that there are many reasons that a call might not connect to the intended party, it is imperative that, when a call is blocked under the authority of the instant Order, the calling party be clearly informed WHY their call has been blocked (e.g., invalid Caller-ID or subject of DNO) and WHO has done the blocking. Any provider in the call path, from the Originating Provider, through one or more intermediate providers, to the Terminating Provider could impose the block. The calling party, a priori, likely does not even know who the entities in the call path are (other than the Originating Provider), let alone which one did the blocking.

Therefore, in our original comments on the NPRM[2], we said: "We propose that, to the extent that the Commission allows (and certainly if it encourages) carriers to block calls, the

[1] Report and Order and Further Notice of Proposed Rulemaking (FCC 17-151, FNPRM), adopted 16 November 2017, available at https://ecfsapi.fcc.gov/file/111717758568/FCC-17-151A1.pdf, para. 57
[2] Comments of ZipDX filed 27 June 2017 ("ZipDX Original Comments") available at https://ecfsapi.fcc.gov/file/10627304016463/ZipDX-17-59-NPRM-NOI-Comments.pdf, page 14

Commission requires … that the block alerts the calling party to the nature of the block and how to resolve it."[3]

The FNPRM asks: "What is the quickest way for callers to be informed of blocking, e.g., should providers send an intercept message to callers to notify them of the block with contact information by which a caller can report and rectify the situation?"[4] The answer to this question is a resounding YES.

More specifically, in those earlier comments, we suggested[5]:

With respect to alerting the calling party, any carrier implementing a block should implement the following:

- *An intercept that identifies the provider implementing the block, informs the caller why their call has been blocked, and gives them contact information allowing both US-based and international callers to reach a live operator 24 hours a day that can, in real time with appropriate explanation, suspend the block. (Virtually all providers are able to play recorded messages when they intercept calls.)*

[3] We note (again) that the Order, taken on its face, could result in extensive false positives particularly with respect to (legitimate) calls from overseas. The Order states: "Because we authorize blocking only for purported NANP numbers, we see no reason why the actual origination point of the call would bear on whether it is blocked. In other words, we find the likelihood of blocking a legitimate call is minimal—no matter its origin." But the Order does not define "purported NANP number." It defines "purport" but does not clarify the NANP/non-NANP distinction. Our knowledge of SS7 suggests that a NANP calling nmber would be a number with the Nature of Address (NOA) set to 0 (and the actual number would then contain 10 digits starting with area code), or NOA would be 4 and the number would start with a 1 followed (normally) by 10 digits. For SIP signaling, the calling number would be a "national" number if it did not start with a "+" (and thus would be a NANP number if on our network), or it could start with a "+1" and that would also be a NANP number. Is that what was intended in the Order? We've stated here the *expected* signaling, but our observation is that many actual calls do not conform (NOA is set incorrectly; or the "+" is not present when it should be, or the "+" is present but the "1" is missing, as examples). As an engineer trying to implement blocking per this Order, and given the vagaries around "purported NANP number" (and "purported non-NANP number"), I don't know how I would determine which calls are candidates for blocking.

[4] FNPRM, para. 57

[5] ZipDX Original Comments, page 15

- *Optionally, callers may be permitted to enter a short sequence of digits or speak a word or phrase that will demonstrate the call is legitimate and allowed to proceed.*

Note that these intercepts are still problematic for those with limited English proficiency, for legitimately-placed automated calls, and for those using TDD, fax or other non-voice communications technologies.

The rules should provide an exception to the intercept requirement when the calling volume is so massive that the carrier is technically unable to play the intercept to all callers.

Our comments also included this[6]:

At 39 and 40, the NOI asks about legitimate callers that find their calls blocked – false positives.

We will address the last items (39/40) first. As noted in the NOI at 39, the terminating provider (that is, the provider serving the call recipient) may not be the one blocking the call. We noted earlier that the Commission must be very explicit about which providers in the call path are allowed to block calls, and what their responsibilities are when they do that. We proposed that if a provider chooses to implement a block, they must provide an intercept message that identifies the provider implementing the block and advises legitimate callers how to lift the block. A provider that cannot comply with this requirement should not block calls except in extenuating circumstances.

Our comments did not, to our knowledge, generate any response in Reply Comments and were not specifically addressed in the final Order.

[6] ZipDX Original Comments, page 23

The FNRPM asks: "[W]e seek comment on ways we can measure the effectiveness of our robocalling efforts as well as those of industry. … Should providers be required to report the quantity of false positives?"[7]

We are not aware of a mechanism whereby a provider could independently KNOW that it had erroneously blocked a call ("false positive") except via a report from some other source. If a provider knows that blocking will result in a false positive, it obviously shouldn't block the call to begin with.

Regarding reporting generally, we would certainly advocate putting reporting requirements on providers if the information collected could be used in some productive way. We have previously commented[8] regarding possible reporting obligations for ORIGINATING PROVIDERS that are allowing large volumes of calls onto the network on behalf of customers where the usage profile matches that of a robocalling campaign. Learning more about such calls could inform Commission and industry positions regarding differentiation between illegal and legal calls and might provide insights for further mitigation efforts.

We aren't sure how other formal metrics regarding blocking of the numbers authorized by the Order would be useful. If, however, the Commission were to convene regular workshops to address the ongoing illegal robocall problem, informal reports from participating providers could certainly prove interesting.

[7] FNPRM, para 59

[8] See our written ex parte comments filed 26-October 2017, available at https://ecfsapi.fcc.gov/file/1026001803270/ZipDX-17-59-WrittenExParte-Oct2017.pdf, Appendix A ("Reporting Requirements") at page 20.

We suspect that imposing reporting requirements on providers that block calls will just further discourage providers from implementing any blocking.

The FNPRM also asks: "Are there other Commission or third-party data sources that the Commission could use to assess the effectiveness of its efforts as well as industry's at targeting illegal robocalls?"[9]

We note that the Federal Trade Commission (FTC) collects consumer complaints about illegal robocalls and do-not-call violations and appears to take those in at a rate roughly ten times that of the FCC. The FTC database would appear to be a potentially valuable resource here. We are not aware of the degree to which the FCC and the FTC cooperate in the complaint collection process and share relevant data. The FCC does not appear to reference the FTC data in any of your documents, but it's hard to believe that you aren't familiar with it.

Another source is the YouMail Robocall Index. Apparently, the FCC is somewhat familiar with this one.[10] One particularly attractive aspect of the data held by YouMail is that it includes audio recordings of the messages left by the robocallers. This can eliminate the hearsay factor when trying to determine the veracity of a robocall complaint; in many cases, the audio content leaves no doubt about the illegality of a call. One would think this could be invaluable to the FCC Enforcement Bureau.

Calculating the extent of the illegal robocall problem network-wide by extrapolating from either of these relatively small-sample datasets introduces a significant measure of uncertainty. We would question the absolute accuracy of any such calculation. However, watching these

[9] FNPRM, para 59

[10] FPNRM, Statement of Commissioner Clyburn, page 51 (with attribution); Statement of Commissioner Rosenworcel, page 54 (without attribution)

numbers month-to-month and year-to-year can certainly give useful trend information. Care should be taken to note any external factors that might influence the underlying collection mechanisms.

Notwithstanding those considerations, we think the FCC should set a publicly stated goal of seeing robocall complaints (as evidenced by the above or similar metrics with historical data available) to 67% of year-end 2017 levels by January 1, 2019 and to 33% of year-end 2017 levels by January 1, 2020.

Deeper analysis of datasets from these sources, and others like them, can provide insight about other trends, such as use of neighbor spoofing.

Knowing that robocallers are often smart and adjust their tactics to evolving defenses, we recommend that the FCC embrace a nimble approach that engages providers and other experts on a less-formal basis (e.g., workshops) where new techniques and fresh data can be exchanged freely.

In closing, we appreciate the FCC's attention to matters of illegal robocalls. However, we have not been bashful in stating that the allocation of Commission and industry resources is suboptimal. We have pointed out that the instant Order is unlikely to produce any lasting, measurable affect on the number of illegal robocalls on our network.

We are also unhappy about the apparent tilting of the tables in favor of the illegal robocallers, and against the white-hat providers that are attempting to mitigate the problem and against the consumers that continue to put up with this scourge.

The Commission is scaring providers with admonishments like "A provider that erroneously blocks calls purporting to originate from allocated numbers may be liable for violating the call

completion rules."[11] There are well-meaning providers that want to make good-faith efforts to combat robocalling, but there may be a small risk of some collateral damage in the form of erroneously blocked calls while algorithms are tested and refined. Yet given the Order's language, no attorney will let their provider client even attempt such a thing when there is a finite risk of violating a stated FCC rule.

The Commission needs to tilt the table in the other direction, encouraging well-intentioned providers to take steps to fight the good fight against the rule-breakers. At the same time, and even more importantly, the Commission needs to hold accountable those few providers that are enabling and in some cases *encouraging* illegal robocallers. Why don't you make THOSE providers liable for violating do-not-call and Truth-in-Caller-ID rules? In separate filings, we will continue to advocate, as we have, for efforts in this direction.

Respectfully submitted,

DATED: 22 January 2018

/s/ David Frankel

dfrankel@zipdx.com
Tel: 800-372-6535

[11] FNPRM, para 31